Universidad Zaragoza
1542

Trabajo Fin de Grado

Observación y análisis de un proyecto real de Big Data desarrollado por el Instituto Tecnológico de Aragón desde la perspectiva de la protección de datos.

Autora

Irene Gómez Polo.

Director

José Félix Muñoz Soro.

Facultad de Derecho, Universidad de Zaragoza

2019.

ÍNDICE:

LISTADO DE ABREVIATURAS USADAS:

1. Instituto Tecnológico de Aragón (ITAINNOVA).
2. Ley Orgánica de Protección de Datos (LOPDGDD)
3. Reglamento General de Protección de Datos (RGPD)
4. Agencia Española de Protección de Datos (AEPD)
5. Servicios de Redes Sociales (SRS)

I. INTRODUCCIÓN:

1. CUESTIÓN TRATADA EN EL TRABAJO DE FIN DE GRADO.

En 2004 la cadena minorista de supermercados Walmart, echó un vistazo al contenido de sus gigantescas bases de datos de antiguas transacciones para comprobar que artículo había comprado cada cliente y su coste total, la hora del día e incluso el tiempo que hacía cuando lo compró; observó con ello que antes de un huracán no solo aumentaban las ventas de linternas sino también las de Pop-Tars, un dulce para el desayuno, desde entonces cuando se avecinaba una tormenta, Walmart colocaba cajas de Pop-Tars en la parte frontal de las tiendas junto a los básicos para huracanes, aumentando así la cantidad de ventas de este dulce [1].

Entre estas dos premisas, el ser humano no es capaz de detectar la existencia de correlación alguna y no hubiera habido forma de saber que a los consumidores les gusta comer Pops-Tars cuando se acerca un huracán sin el análisis de estos datos. Entonces, ¿qué pasaría si tuviéramos una fuente de infinitos datos?, podríamos establecer relaciones inexplicables, como la que descubrió Walmart, en casi todos los ámbitos de nuestra vida. Pues bien, esa fuente existe y la llamamos Internet.

Dentro de él una de las protagonistas son las plataformas de redes sociales, las redes sociales permiten a sus usuarios crear contenidos de manera sencilla, expresar su opinión sobre los contenidos generados por otros usuarios, referenciar páginas web y documentos y, en general, difundir aquello que es de su interés. Las aplicaciones de acceso a las redes sociales permiten incorporar a los contenidos generados por el usuario datos capturados por los sensores que incorporan sus dispositivos: el lugar de residencia del mismo, el lugar desde el que se está generando el contenido o el recorrido que ha realizado durante un paseo. Analizar estos elementos intangibles de nuestra vida diaria, permite transformar los datos en información y conocimiento con un potencial extraordinario. Por ejemplo:

Una serie de empresas hizo un estudio sobre el uso de redes sociales, y el tráfico de información que se producía en las mismas como señales que permitieran establecer valoraciones crediticias. La idea base de su estudio fue <<Dios los cría y ellos se juntan, las personas prudentes hacen amistad

[1] V. MAYER - SCHÖNBERGER y K. CUKIER, Big data. La revolución de los datos masivos, Titivillus, 2013, p. 36.

con gente de mentalidad parecida, mientras los derrochadores incurren juntos en el impago>>, así que Facebook podría ser la próxima empresa en darnos una lista de posibles morosos [2].

Vamos a imaginar ahora que Walmart en vez de usar las bases de datos de antiguas transacciones hubiera usado un algoritmo que le permitiera ver los comentarios de la gente en Twitter sobre sus productos, y en concreto sobre los dulces Pop-Tars, posiblemente hubiera encontrado varios tweets con expresiones como <<¡Que bien se está en casa comiendo Pops-Tars mientras llueve fuera!>>. Hubiera llegado entonces a la misma conclusión que analizando todas sus antiguas transacciones, y solo hubiera necesitado un clic de ratón.

Pues lo expuesto en este último ejemplo es lo que hace en la realidad el Instituto Tecnológico de Aragón (ITAINNOVA), apoyando a empresas e instituciones en su desarrollo económico mediante la innovación en el ámbito de las tecnologías y en concreto del Big Data, y usando las redes sociales como fuente de información.

En su camino de desarrollo del Big Data, y el tratamiento de datos, su deseo es adaptarse completamente a la normativa vigente en materia de protección de datos, y esta es la ayuda que yo les voy a proporcionar con mi investigación y posterior desarrollo del siguiente Trabajo de Fin de Grado (TFG).

2. RAZÓN DE LA ELECCIÓN DEL TEMA Y JUSTIFICACIÓN DE SU INTERÉS.

Elegí este tema por varios motivos:

En primer lugar por tratarse de un caso real, ya que no consiste únicamente en estudiar una materia de forma teórica, sino que me permite analizar un proyecto que se está desarrollando actualmente, conocer el funcionamiento de nuestro derecho, y en concreto de las normas relativas a protección de datos, desde un punto de vista práctico.

Por otra parte se trata de ayudar a una entidad, como es ITAINNOVA, a que pueda llevar a cabo su trabajo sin salirse de las lineas marcadas por nuestro ordenamiento jurídico, lo que despierta en mí un mayor interés y entrega a la hora de investigar.

[2] Ibídem, p. 60.

Por último elegí esta cuestión, por la rama del derecho que es marco de esta investigación, la protección de datos personales, pues tal y como marca la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) en su preámbulo, <<Internet, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. (…) Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía >>.

Observamos entonces que un uso de las oportunidades brindadas por Internet (como el Big Data) lleva consigo unos riesgos, que en ocasiones suponen la vulneración de los derechos fundamentales que establece la Constitución Española en su artículo (art.)18.

<<**1.** Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
(….)
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos >>.

Yo misma, como usuaria de Internet y redes sociales, tengo interés en la protección de mis datos personales, pero también en que estos puedan ser útiles a la hora de innovar en el ámbito del marketing empresarial. Por esto y por tratarse de un proyecto actual donde puedo proporcionar ayuda a una entidad real concluyo mi interés por el tema elegido.

3. METODOLOGÍA SEGUIDA EN EL DESARROLLO DEL TRABAJO.

El objetivo del trabajo es ayudar a ITAINNOVA, en el aspecto legal de la protección de datos, en el desarrollo de la plataforma de prototipado rápido de aplicaciones de Big Data a Inteligencia Artificial, denominada Moriarty. Aunque nos referiremos a ella como Moriarty en el resto del documento, el análisis que realizamos se centrará en Social Moriarty, que es el nombre con que ITAINNOVA se refiere al subconjunto de funcionalidades de Moriarty que se aplican a la captura, análisis y visualización de los datos obtenidos en redes sociales.

Para cumplir este objetivo he concertado reuniones con los responsables de Moriarty, con el tutor de mi trabajo, y he investigado sobre el tema tanto en Internet como a través de diferente bibliografía. En las reuniones concertadas con ITAINNOVA el 17 de enero de 2019, y el 7 de marzo de 2019, donde en concreto me atendieron Rafael Del Hoyo y Francisco José Lacueva, responsables del proyecto, me mostraron la actuación del programa y me proporcionaron la guía de funcionamiento del mismo. Con estos datos, fuí solicitándoles aclaraciones sobre el funcionamiento de las distintas partes del programa, a la vez que ellos me transmitían las dudas legales que tenían con respecto a su tratamiento. Sobre esta base, el tutor de mi TFG me ayudó a diseñar la estructura del trabajo, definiendo los puntos esenciales que deberían observarse siempre en un tratamiento de datos. A partir de ahí, he ido elaborando el trabajo de la siguiente manera: sobre cada uno de los apartados del índice, he recabado toda la información posible que me fuese útil, primero en la ley, y posteriormente en bibliografía, jurisprudencia e Internet. Una vez obtenidos todos estos datos, he intentado adaptarlos al tratamiento que lleva a cabo ITAINNOVA, concretando con ellos las actuaciones que realizan relativas a cada apartado, y confirmando con mi tutor la aplicación de la ley a estas actuaciones en concreto.

En todos esos puntos he intentado realizar un supuesto mental de las actividades de ITAINNOVA y comprobar cómo se adaptaban a las propuestas de la ley. Esto me ha supuesto una gran complicación teniendo en cuenta que el nuevo RGPD comenzó a ser aplicable a partir del 25 de mayo de 2018 y que todavía no hay suficiente jurisprudencia, ni doctrina sobre algunos de los cambios que ha producido. Por lo que he ido recopilando aquellas actividades que generasen dudas sobre su legalidad para comentarlas posteriormente con mi tutor y resolverlas gracias a su asesoramiento y la bibliografía consultada.

II. ¿QUÉ ES EL INSTITUTO TECNOLÓGICO ARAGONÉS Y CUAL ES SU TRABAJO?

Tal y como se define en su propia pagina web, ITAINNOVA es <<Un centro tecnológico con personalidad jurídica propia, sin animo de lucro y cuyos fines son de interés general, legalmente constituido a iniciativa del Gobierno de Aragón en 1984 y presidido por el Departamento de Innovación, Investigación y Universidad del Gobierno de Aragón que cuenta así mismo con el reconocimiento del Ministerio de Economía y Competitividad como Oficina de Transferencia Tecnológica (…). La misión de ITAINNOVA es ayudar a las empresas y promover las posibilidades

tecnológicas de esta región, para desarrollar nuevos productos y procesos, con el propósito de impulsar la competitividad en la Unión Europea…>> [3]

Entre las tecnologías promovidas por ITAINNOVA esta el Big data, la ciencia que trata de recopilar datos a gran escala y extraer de ellos una información útil y que aporte conclusiones eficaces para el desarrollo social y empresarial. A continuación voy a estudiar este almacenamiento y análisis de datos desde la perspectiva jurídica de la protección de datos digitales, examinando concretamente el siguiente proyecto de Big data creado por ITAINNOVA

III. PROYECTO BASE DEL TFG: MORIARTY.

Moriarty es el nombre de la plataforma para el prototipado rápido de aplicaciones de Big Dada desarrollada por ITAINNOVA con la siguiente finalidad: <<Moriarty ayuda a resolver diferentes problemáticas de negocio con grandes volúmenes de datos. Además, permite entender y estructurar la información, identificar patrones y correlaciones ocultas en los datos, inducir conocimiento, y construir sistemas de aprendizaje. El gran valor que Moriarty ofrece es que posibilita la conversión de datos en valiosa información, de manera ágil, precisa y sencilla, facilitando la toma de decisiones estratégicas. Además su capacidad para utilizar técnicas avanzadas de análisis semántico le otorga un valor diferencial que hace de Moriarty una herramienta única>>.[4]

Como mencionábamos previamente, Moriarty permite crear sistemas informáticos que analizan el contenido generado en redes sociales para distintas empresas. Los sistemas desarrollados capturan datos de las redes sociales, los analizan mediante algoritmos inteligentes, y permiten visualizarlos de manera gráfica junto con la información y conocimiento generado por los algoritmos. Es la visualización la que aporta valor a las empresas para las que se desarrollan. La utilización de distintos componentes gráficos permite destacar patrones diferentes en los datos de interés y, en consecuencia, facilitan la extracción de conclusiones de manera sencilla para soportar la toma de decisiones. Una vez desarrollado el sistema informático, la empresa contratante se convierte en propietaria del mismo, en particular, del repositorio de datos creado, obteniendo así una herramienta de soporte a sus actividades diarias.

---

[3] Página web de ITAINNOVA: https://www.itainnova.es/es/itainnova. Consultada el 25 de marzo de 2018

[4] Ibídem.

Vamos a ver un ejemplo:

Una empresa contrata a ITAINNOVA para observar la reputación que tiene su producto A en Aragón, ITAINNOVA crea un fichero de datos especifico para este tema, extrayéndolos de las redes sociales en forma de comentarios, este fichero se analiza mediante un sistema informático que busca en él conceptos relativos a ese producto A en Aragón. Las conclusiones que obtendríamos mediante estadísticas podrían ser las siguientes:

Imagen 1: Nube de conceptos, palabras más nombradas en las redes sociales junto al producto A.

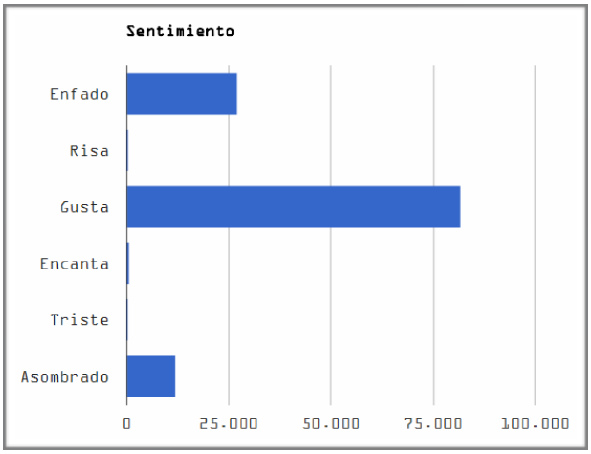

Imagen 2: Sentimientos generales de los documentos (Tweets, comentarios, menciones en redes sociales) obtenidos respecto del producto A en Aragón.

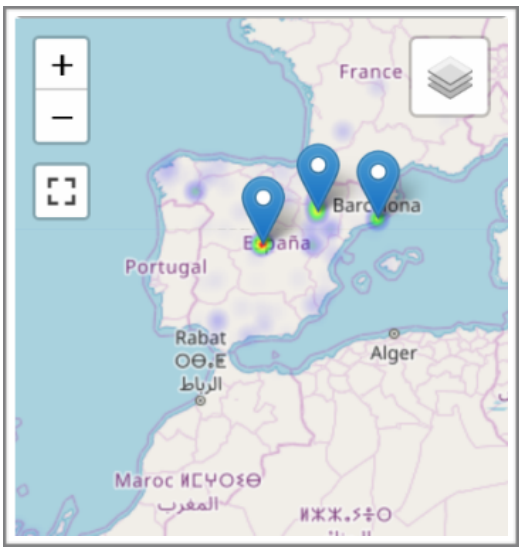

Imagen 3: Visualización de la distribución de documentos filtrados por provincias, desde que provincias se ha hablado más sobre el producto.

Una vez tenemos estas imágenes, entre muchas otras, Moriarty permite analizar cuales son los documentos (como un tweet) que han creado las estadísticas, es decir, pincharemos en el sentimiento <<Gusta>> de la gráfica de sentimientos y podremos ver cuales son los comentarios concretos en redes sociales que han creado ese sentimiento hacia el producto. Podemos ver cada comentario de la red social tal y como está, con nombres y apellidos e incluso dirigirnos al perfil de la persona que lo ha escrito.

Estas gráficas, junto con la lectura de los documentos y el descubrimiento de qué personas hablan sobre el producto, permiten a las empresas la creación de grandes estrategias comerciales adaptadas a nuestras necesidades de consumo, y a la mejora de sus productos para triunfar en el mercado. Pero Moriarty no solo trata de llegar a estas conclusiones, sino que es un sistema completo; en él podemos buscar mucha más información mediante un sistema de filtrado, pues entre los datos recogidos no están solo los relativos al producto A, sino muchos otros que ITAINNOVA ha considerado que podrían ser útiles para la empresa. Imaginemos que posteriormente la empresa necesita saber lo que se está hablando sobre el producto B, pues bien, para ello no haría falta crear un nuevo sistema porque hayamos cambiado de producto, sino cambiar los filtros de búsqueda en Moriarty y los algoritmos se pondrían a funcionar obteniendo nuevas gráficas y conclusiones.

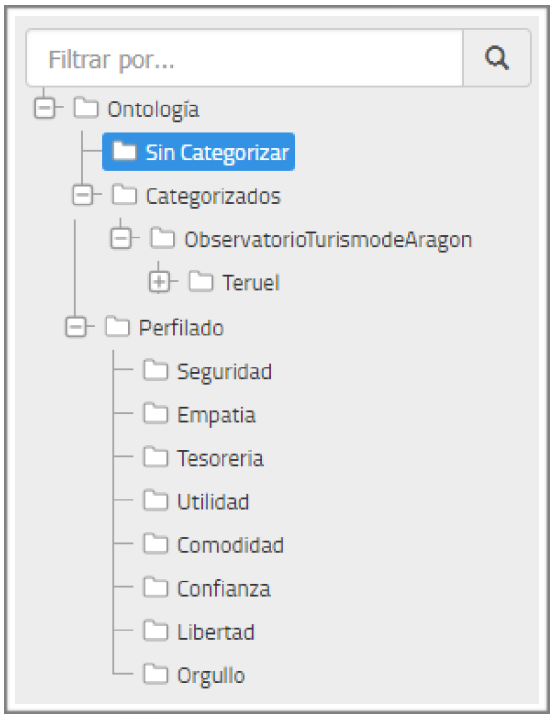

Imagen 4: Ejemplo de sistema de filtrado para hacer búsquedas dentro del programa.

Debo aclarar que el servicio de ITAINNOVA no es solo la búsqueda de información en Moriarty, sino la creación de un fichero de datos específicos para cada cliente, poniéndolos a su disposición junto con el programa informático que le permitirá la búsqueda en el fichero de la información que necesite en cada momento.

IV. TRATAMIENTO DE DATOS LLEVADO A CABO EN ESTE PROYECTO.

1. QUIÉN TRATA LOS DATOS Y POR ENCARGO DE QUIÉN.

Para ver este punto, primero debemos determinar qué se considera tratamiento de datos y esto lo determina en su art. 4 el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos (RGPD):

<<tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción,

consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción>>

Por tanto realizan un tratamiento de datos todas aquellas personas que lleven a cabo alguna de estas operaciones sobre datos personales, en concreto, en nuestro proyecto podemos entender que ITAINNOVA y la empresa que les contrata efectúan un tratamiento de datos conjuntamente, pero que dentro de esta acción cada uno desempeña una función diferente que derivará, en caso de incumplimiento de la ley, en responsabilidades diferentes.

Para identificar qué papel ejercen estos dos actores en Moriarty vamos a ver primero cuales son los posibles sujetos existentes en un tratamiento de datos. El art. 4 del RGPD define los siguientes:

<<responsable del tratamiento o responsable: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento…>>

<<encargado del tratamiento o encargado: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento >>

<<destinatario: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero…>>

Además de estas tres figuras, de la definición de datos personales podemos extraer el concepto de interesado, <<Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona>>. Será por tanto interesado el titular de los datos que están siendo tratados, siempre que sea persona física identificada o identificable.

Una vez definidos los conceptos vamos a ver cuál de ellos corresponde a cada uno de los actores participantes en Moriarty: esta claro que el afectado o interesado será la persona física titular de datos, es decir la persona a la que correspondan los tweets, comentarios en Facebook y demás

documentos usados en Moriarty para la creación de estadísticas y conclusiones. Sabemos también que el destinatario que se beneficiará finalmente del tratamiento de esos datos será la empresa, ya que a ella se le comunicarán o podrá obtener las conclusiones, estadísticas y documentos finales seleccionados. Por último, la parte más discutible es definir quién es el encargado del tratamiento y quién el responsable del mismo.

En el Dictamen 1/2010, adoptado el 16 de febrero de 2010 por el Grupo de Trabajo del artículo 29 sobre protección de datos de la Directiva 95/46/ CE, se explican de forma detallada los conceptos de «responsable del tratamiento» y «encargado del tratamiento». Antes de entrar a analizarlo debo clarificar que esta Directiva fue derogada el 25 de mayo de 2018 por el nuevo RGPD, pero que las definiciones que da sobre responsable y encargado del tratamiento en su art. 2.d y e, han sido mantenidas en el art. 4 del RGPD, que es la norma actualmente en vigor. Una vez aclarado esto paso a exponer lo que dice el Dictamen 1/2010 sobre estas figuras controvertidas:

<<El concepto de responsable del tratamiento es autónomo, en el sentido de que debe interpretarse fundamentalmente con arreglo a la legislación comunitaria de protección de datos, y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal. La definición de la Directiva consta de tres componentes fundamentales:

- el aspecto personal («la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo»);

- la posibilidad de un control plural («que solo o conjuntamente con otros»);

- Y los elementos esenciales para distinguir al responsable del tratamiento de otros agentes («determine los fines y los medios del tratamiento de datos personales»)

(…)

Este dictamen analiza también el concepto de encargado del tratamiento, cuya existencia depende de una decisión adoptada por el responsable del tratamiento, que puede decidir que los datos se traten dentro de su organización o bien delegar todas o una parte de las actividades de tratamiento

en una organización externa. Para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste>>[5]

El elemento esencial de la definición de responsable del tratamiento es el tercer componente de la misma, lo que, desde mi punto de vista, es la parte delimitante de las dos figuras, <<Este tercer elemento representa la parte sustantiva de la prueba: lo que una parte debe determinar para que se la pueda considerar responsable del tratamiento. (…)
A la hora de evaluar la determinación de los fines y los medios con vistas a asignar la función de responsable del tratamiento, la pregunta crucial que se plantea por tanto es hasta qué nivel de detalle debe determinar una persona los fines y medios para que se la considere responsable del tratamiento.>>[6]

En Moriarty es la empresa contratante quien determina los fines del tratamiento, al ser la que contrata a ITAINNOVA con un fin específico: analizar lo que sobre ella o sobre un producto suyo se dice en la red. Podría albergarse alguna duda respecto a quién determina en Moriarty los medios por los que se lleva a cabo el tratamiento, pero el Dictamen 1/2010 salva esta incertidumbre describiendo lo siguiente:

<<La determinación del «fin» del tratamiento es competencia del «responsable del tratamiento». Por consiguiente, quienquiera que tome esta decisión es (de facto) el responsable del tratamiento. Éste puede delegar la determinación de los «medios» del procesamiento en la medida en que se trate de cuestiones técnicas u organizativas. Las cuestiones de fondo que sean esenciales a efectos de la legitimidad del tratamiento son competencia del responsable del tratamiento>>[7]

En suma, y considerando que ITAINNOVA se dedica a la creación del programa mediante sus propios criterios pero que este será usado siguiendo directivas de la empresa contratante, podemos concluir lo siguiente, los sistemas informáticos desarrollados usando Moriarty son proyectos donde el tratamiento de datos es llevado a cabo conjuntamente, entre el cliente que es el contratante e

[5] Grupo de Trabajo del art. 29, Dictamen 1/2010, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»,16 de febrero de 2010. p. 1.

[6] Ibídem, p. 13 y 14.

[7] Ibídem, p. 16.

ITAINNOVA que es el contratado, pero desempeñando funciones distintas, la empresa lo hace como responsable del tratamiento e ITAINNOVA como encargado del mismo, las responsabilidades que de estas funciones se puedan derivar y la relación que se establece entre ambos sujetos será objeto de análisis del apartado V.5.3.

2. QUÉ TIPO DE DATOS SON TRATADOS.

Según la definición de tratamiento que da el RGPD para que este exista, debe ser siempre sobre datos personales, la palabra personales tiende a hacernos pensar en datos íntimos de la vida de una persona, pero la realidad es que la categoría "datos personales" engloba como define el RGPD <<toda información sobre una persona física identificada o identificable («el interesado»)>>.

ITAINNOVA trata datos de carácter personal, ya que recoge información que ha sido publicada directamente por los usuarios en las redes sociales y que estos usuarios son perfectamente identificables con Moriarty, pues incluso podemos entrar en sus perfiles personales.

Diferenciamos dentro de los datos personales un tipo de datos especialmente protegidos, que dada su importancia la ley no permite tratar salvo en determinadas excepciones, estas son las llamadas categorías especiales de datos. Veamos la base legal que nos permitirá tratar cada tipo de datos:

2.1 DATOS PERSONALES NO INCLUIDOS EN LAS CATEGORÍAS ESPECIALES DE DATOS:

La base legal que nos permite llevar a cabo un tratamiento de datos personales la proporciona el Artículo 6 del RGPD 2016/679 que es el que nos habla de "la licitud del tratamiento":

<<El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- el interesado dió su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

- el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
- el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño>>

Parece obvio que de los puntos anteriores, solo dos podrían servir a ITAINNOVA para justificar su tratamiento de datos: la satisfacción de intereses legítimos o el consentimiento. Analicemos ambos:

A. INTERÉS LEGÍTIMO:

La satisfacción de intereses legítimos autoriza el tratamiento de datos, siempre que se cumplan una serie de condiciones. Debemos pues analizar si esta base legal permite a ITAINNOVA tratar los datos de redes sociales que almacena y usa en Moriarty.

Debemos plantearnos tres puntos: ¿cuál es el interés que tiene ITAINNOVA?, ¿es ese interés legítimo?, y si lo es, ¿sobrepasa los intereses, derechos y libertades de aquellos a quien pertenecen los datos?.

Respecto al interés de ITAINNOVA y el cliente, a quien proporcionara los datos y el programa, sabemos lo siguiente: <<Moriarty ayuda a resolver diferentes problemáticas de negocio con grandes volúmenes de datos (Big Data). Además, permite entender y estructurar la información, identificar patrones y correlaciones ocultas en los datos, inducir conocimiento, y construir sistemas de aprendizaje.>>[8]

[8] www.itainnova.es Consultada a 31 de mayo de 2019.

Por tanto el interés de los mismos es la toma de decisiones estratégicas respecto a una serie de productos, para modificar sus cualidades y adaptarlos a un mercado que expresa lo que le gusta, y lo que no, en las redes sociales.

La legitimidad de este interés viene determinada por lo que expresa el Grupo de Trabajo sobre Protección de Datos del art. 29 en su Dictamen 06/2014 relativo al concepto de interés legitimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE. Debo aclarar que esta Directiva fue derogada por el RGPD 2016/679, pero que el interés legítimo ha sido mantenido en el art. 6.1.f del Reglamento, actualmente en vigor, como base legal para el tratamiento de datos, al igual que lo hacia el art. 7.f de la citada Directiva, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

Continuando entonces con el Dictamen del Grupo de Trabajo del Artículo 29 considero el interés de ITANNOVA, y de la empresa, como legítimo, ya que es real, suficientemente específico, y legal conforme a la legislación nacional y europea. Incluso está incluido, como legítimo, en una lista no exhaustiva que este grupo da en su dictamen: <<tratamiento con fines de investigación (incluida la investigación de mercados)>>. Además si la empresa decidiera posteriormente a esta investigación, llevar a cabo publicidad estratégica con la información recabada, seguiría siendo este un interés legítimo, pues también esta incluida la opción de comercialización o publicidad en la lista que da el Grupo de Trabajo sobre el concepto de interés legítimo del responsable del tratamiento de los datos.[9]

Y por último, el que el interés sea legítimo autoriza a tratar datos personales al amparo del art. 6 del Reglamento, pero este artículo también nos obliga a contraponer el interés legítimo a los intereses, derechos y libertades fundamentales de aquellos a quien pertenecen los datos tratados, en nuestro caso, los usuarios de redes sociales de los que se han obtenido los datos. Podemos ver que la ley

---

[9] Grupo de Trabajo del art. 29. Dictamen 06/2014 sobre el concepto de interés legitimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, 9 de abril de 2014. p.30.

<<por tanto, un «interés legítimo» que sea pertinente en virtud del artículo 7, letra f), debe:

-ser lícito (es decir, de conformidad con la legislación nacional y de la UE aplicable);

-estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se lleve a cabo en contraposición a los intereses y los derechos fundamentales del interesado (es decir, suficientemente específico);

-representar un interés real y actual (es decir, no especulativo)>>

prevé un plus de protección al usuario al incluir sus intereses, <<La referencia a los «intereses o derechos y libertades fundamentales» (…) prevé más protección al interesado, es decir, exige que se tenga en cuenta también el «interés» de los afectados, no solo sus derechos y libertades fundamentales>>[10]. Además debemos pensar que en el caso de los interesados no se incluye el adjetivo legítimo, lo que conlleva un ámbito mas amplio de protección de sus derechos e intereses que no podrá traspasarse, ni si quiera cuando estos estén implicados en actividades ilegales.

¿Cómo podemos valorar que el tratamiento no rebasa los intereses, derechos y libertades fundamentales del interesado? <<Los Estados miembros han definido una serie de factores útiles que deben considerarse al efectuar la prueba de sopesamiento (…):

- Evaluación del interés legítimo del responsable del tratamiento;
- Impacto sobre los interesados;
- Equilibrio provisional
- Garantías adicionales aplicadas por el responsable del tratamiento para impedir cualquier impacto indebido sobre los interesados>>[11]

Según estos cuatro puntos, para llevar a cabo la contraposición deberíamos primero conocer cual es la finalidad de nuestro interés legítimo, la cual ya se ha indicado arriba, y en segundo lugar ver el impacto que tiene el tratamiento en los intereses, derechos y libertades del interesado analizando lo siguiente: <<la naturaleza de los datos personales, la manera en que se trata la información, las expectativas razonables de los interesados, y la posición del responsable del tratamiento y del interesado. También se debatirán brevemente cuestiones relativas a las fuentes potenciales de riesgo que puedan dar lugar a repercusiones para las personas implicadas, la gravedad de estas, y la probabilidad de que dichas repercusiones se materialicen>>[12]

De acuerdo con el Grupo de Trabajo del art. 29 el impacto para los interesados es un concepto mucho más amplio que el daño o perjuicio, sin embargo respecto al tratamiento que realiza ITAINNOVA el impacto es mínimo, ya que como veremos más adelante los datos que trata no son especialmente protegidos, además se van a utilizar para crear estadísticas que ayuden en la toma de

[10] Ibídem, p. 35.

[11] Ibídem. p.39 y 40.

[12] Ibídem p.43

decisiones, pero no serán usados para la creación de perfiles que permitan hacer predicciones o modificar comportamientos. Y en relación a las expectativas de los interesados, y a la posición del responsable del tratamiento e interesados, aunque estos últimos desconocen el proyecto, las fuentes potenciales de riesgo que podría haber respecto a sus intereses, derechos y libertades se ven minorizadas ya que el tratamiento de datos practicado por ITAINNOVA se reduce a utilizar los tweets o comentarios, que los mismos interesados han publicado en las redes sociales, para la creación de gráficas, convirtiendo estos datos en números estadísticos.

En cuanto al almacenamiento de esos datos en un fichero, al estar este desconectado de Internet su situación es mucho más segura, reduciéndose el posible impacto sobre los interesados tal y como indica el Grupo de Trabajo mencionado <<Un sistema estable y homogéneo que no tenga interconexiones y esté desconectado de Internet conlleva una probabilidad mucho menor de poner en peligro la seguridad de los datos>>[13]

Respecto a los dos últimos puntos, el equilibrio provisional nos indica que cumpliendo las obligaciones que establece el Reglamento para el responsable y encargado, será menos probable que haya una injerencia en los intereses, derechos y libertades de los interesados, y normalmente el interés legítimo nos servirá como base legal al tratamiento de datos; no obstante, el cumplimiento de estas obligaciones no siempre garantiza que los intereses, derechos y libertades de los usuarios no se vean mermados, y será en estas ocasiones cuando habrá que añadir las garantías adicionales que nos muestra el último punto.

Pero además de los cuatro puntos anteriores, hay que tener en cuenta que el tratamiento de los datos debe ser proporcionado y necesario para conseguir el fin propuesto, por lo que al comparar este interés legítimo del responsable y el encargado, y los intereses y derechos de los interesados, debemos comprobar que los datos personales y el tratamiento de los mismos sean necesarios para el interés legítimo que autoriza a los primeros, pues si los datos obtenidos o el tratamiento de los mismos no están enfocados a la realización del fin declarado por el responsable y el encargado, se habrán sobrepasado los intereses y derechos de los interesados, no habiendo base legal para tratar sus datos.

[13] Ibídem, p.45.

Una vez comprobado que ITAINNOVA y su cliente tienen un interés legítimo y que el impacto sobre los intereses, derechos y libertades de los interesados es mínimo, se crea una base legal que permite a ITAINNOVA el tratamiento de datos personales no incluidos en la categoría de especialmente protegidos.

B. CONSENTIMIENTO:

Veamos si además del interés legítimo existe otra base legal que nos autorice al tratamiento de estos datos, sería el consentimiento que en su caso hubiera prestado el interesado. Según la Guía del RGPD creada por la AEPD <<El consentimiento inequívoco es aquel que se ha prestado mediante una manifestación del interesado o mediante una clara acción afirmativa>>[14].

ITAINNOVA no tiene consentimiento de los usuarios para tratar sus datos personales, pues estos no se lo han otorgado directamente, y lo más probable es que ni si quiera sepan que se esta usando la información que publican en redes sociales como objeto de tratamiento. Es cierto que cuando alguien se hace un perfil en una red social da su consentimiento al tratamiento de los datos personales que allí sean publicados, pero a quien consiente que haga el tratamiento es a la red social; y ese consentimiento no puede delegarse infinitamente a diferentes empresas o entidades que trabajen con lo publicado en redes sociales, de lo contrario estaríamos concediendo un permiso ilimitado al tratamiento de nuestros datos.

2.2 DATOS PERSONALES QUE SÍ ESTÁN INCLUIDOS EN LAS CATEGORÍAS ESPECIALES DE DATOS:

No existe una definición como tal de los mismos pero el art. 9 del RGPD 2016/679 los enumera, siendo los siguientes:

<<Los que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.>>

[14] Guía del Reglamento General de Protección de Datos para responsables de tratamiento [e-Book] Madrid, Agencia Española de Protección de Datos, 2017, p.6

El art. 9 impide el tratamiento de este tipo de datos, a no ser que nos encontremos en una de las siguientes situaciones:

- << si el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.
- Si el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos, (…);
- Si el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, (…);
- Si el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, (…);
- Si el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
- Si el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones (…);
- Si el tratamiento es necesario por razones de un interés público esencial, (…);
- Si el tratamiento es necesario para fines de medicina preventiva o laboral, (…);
- Si el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, (…),
- Si el tratamiento es necesario con fines de archivo en interés público, (…)>>

Así pues necesitaremos que se dé, en el contexto de Moriarty, una de estas excepciones para poder tratar datos de este tipo. Podemos observar que entre los supuestos que nos podrían permitir el tratamiento de datos especialmente protegidos no se encuentra el interés legítimo que autorizaba a ITAINNOVA a tratar datos personales no incluidos en esta categoría. Solo dos de las excepciones allí recogidas podrían permitirnos tratar este tipo de datos:

A. CONSENTIMIENTO EXPLÍCITO:

El consentimiento explícito como base legal en el caso de los datos especialmente protegidos es mucho más exigente que cuando estos no lo son, ya que hay que tener en cuenta que el art. 9.1 de la LOPDGDD 3/2018 establece con respecto a este punto que, en derecho español, es necesario además de ese consentimiento del interesado la concurrencia de otra de las excepciones que nos da el 9.2 RGPD: <<Categorías especiales de datos. 1. A los efectos del art. 9.2 a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico>>

Hemos determinado anteriormente que ITAINNOVA no había obtenido un consentimiento expreso por parte de los usuarios que le permitiera el tratamiento de sus datos, por lo que no podemos basarnos en esta excepción para permitir el tratamiento de datos personales especialmente protegidos, y más siendo en este tipo de datos necesaria, ademas del consentimiento, la concurrencia de otra excepción.

B. QUE EL INTERESADO HAYA HECHO ESOS DATOS MANIFIESTAMENTE PÚBLICOS:

Anteriormente a la entrada en vigor del RGPD, la AEPD había determinado en numerosas ocasiones que una publicación manifiesta se consideraba como <<un supuesto de consentimiento inequívoco manifestado de forma tácita. Es decir, parece que la AEPD equipara el supuesto de los datos que se hayan hecho manifiestamente públicos al consentimiento tácito>>[15].

Sin embargo uno de los grandes cambios del RGPD fue la eliminación del consentimiento tácito como base legal al tratamiento de datos, así podemos verlo en el punto V del Preámbulo de la LOPDGDD, que desarrollando el Reglamento, aclara lo siguiente sobre el consentimiento <<que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una

[15] J. A. Messía de la Cerda Ballesteros. Actualidad Civil, Nº 5, 2018. Al que se hace referencia en https://laleydigital.laley.es. LA LEY 4473/2018, consultada el 30 de mayo de 2019.

pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas>>.

Habiendo eliminado el Reglamento como base legal al tratamiento de datos el consentimiento tácito, nos preguntamos ¿por que continua como una de las excepciones para el tratamiento de datos especialmente protegidos el haberlos hecho, por el interesado, manifiestamente públicos? A mi parecer este punto se ha mantenido en la ley únicamente, para datos que son notoriamente públicos, por ejemplo para un político que aparece en las listas electorales de un determinado partido, su afiliación a este partido podría ser considerada en este caso un dato manifiestamente público, y su tratamiento sería legítimo, no por entenderse esa manifestación pública como un consentimiento tácito al tratamiento del mismo, sino porque ese dato es tan sobradamente conocido y tan accesible, que su tratamiento no supondría ningún impacto sobre el interesado.

Por todo lo visto en este punto V.2, podemos determinar que ITAINNOVA y su cliente no pueden tratar datos categorizados como especialmente protegidos, ya que no pueden acogerse a ninguna de las excepciones del art. 9 del RGPD, y únicamente podrán, al amparo del interés legítimo, tratar datos de carácter personal que no están dentro de la categoría de especialmente protegidos, pero además deberán tener en cuenta que este interés legítimo nunca debe sobrepasar los intereses, derechos y libertades fundamentales de los interesados.

La diferenciación de estos tipos de datos no siempre resulta fácil, veremos en el siguiente punto algunos casos en los cuales es difícil discernir si los datos a tratar pertenecen o no a la categoría de especialmente protegidos y si será posible tratarlos en base al interés legítimo.

2.3 DIFICULTAD DE INCLUIR CIERTOS DATOS PERSONALES EN UNA U OTRA CATEGORÍA:

Según los puntos anteriores ITAINNOVA esta autorizada por el interés legitimo para tratar datos de carácter personal que no sean especialmente protegidos, y no lo está para tratar aquellos que sí lo son; pero hay ciertos datos que generan dudas sobre su inclusión o no en la categoría de especialmente protegidos, se trata de datos que aunque a priori parece que no son especialmente protegidos, pueden generar información que sí lo sea.

Por ejemplo, mucha de la información recopilada por ITAINNOVA para las empresas versa sobre alimentos, imaginemos que una empresa solicita un tratamiento de datos sobre carne Halal, ya que es un proveedor de este tipo de carne, entre otras; y quiere saber que se está hablando de ella en Twitter. Halal es una palabra de origen árabe que significa "lícito", se usa por el pueblo islámico para referirse a todas aquellas comidas y actos que son permitidos por la religión musulmana. Es cierto que todo el mundo que habla de carne Halal en Twitter no tiene por qué ser musulmán pero una gran parte seguramente lo sea, y este tratamiento de datos nos revelaría la ideología de muchas de las personas sobre las que se han recopilado tweets.

Para analizar si la recopilación de datos, que a priori no entran dentro de las categorías especiales pero que pueden revelar información especialmente sensibles, es un tratamiento o no de datos especialmente protegidos, añado otro ejemplo relativo al tratamiento de datos de geolocalización: Los datos de localización geográfica son los que permiten indicar la posición en el espacio de un sujeto, así como trazar una linea de sus desplazamientos, estos datos también nos hacen dudar de si deben gozar de una especial protección y considerarse por tanto dentro de la categoría de datos especialmente protegidos, pues, si por ejemplo, podemos localizar a una persona un domingo en una iglesia, deduciremos fácilmente que es católica.

<<La cuestión es entonces determinar si los datos que permitan localizar a una persona han de considerarse especialmente protegidos, pregunta que entiendo debe encontrar una respuesta negativa. Ciertamente, el entrecruzamiento de datos de localización podría conducir a elaborar un perfil de personalidad que arrojara información sobre informaciones especialmente sensibles (salud, ideología, religión, vida sexual, etc.). Sin embargo, el elemento determinante de la consideración de unos concretos datos de carácter personal como «datos sensibles» es que formen parte del objeto de protección propio del derecho a la intimidad o a la libertad religiosa o ideológica, es decir, su vinculación originaria con otros derechos fundamentales distintos del derecho a la protección de los datos de carácter personal (que en todo caso estará implicado). Asignar la categoría de «dato especialmente protegido» a un dato de carácter personal no ha de hacerse depender de los efectos que surta su conexión con otros, pues podríamos caer en el peligro de sobredimensionarla: todos podrían ser en última instancia datos sensibles>>[16]

[16] J. Pérez Gil, Protección de datos y proceso penal, LA LEY, Madrid, 2010. Consultado en: laleydigital.laley.es, LA LEY 8123/2011 a 31 de mayo de 2019.

En base a lo anterior deduzco que si el dato en sí mismo, sin ser relacionado con otros, puede proporcionarnos la información especialmente protegida deberá ser considerado un dato especialmente protegido y tratarse como tal; en cambio, si es necesario poner ese dato en conexión con otros para deducir la información especialmente protegida, no deberá ser categorizado como especialmente protegido y podrá ser tratado bajo la condición del interés legítimo, como cualquier otro dato personal que no sea especialmente protegido. Si fuera de otra forma cualquier dato podría considerarse especialmente protegido, pues en relación con otros es muy posible que nos proporcione un perfil personal del interesado con información relevante sobre su vida íntima.

Concluyo, en base a lo anterior, que si entendemos que el haber hablado de carne Halal determina por si mismo que una persona tiene una ideología musulmana, ese dato será sensible e ITAINNOVA deberá abstenerse de su inclusión en el fichero aunque la empresa se lo solicite, de lo contrario podría incurrir en corresponsabilidad, pues no tienen base legal para su tratamiento. Por el contrario, si aceptamos que haber hablado de este tipo de alimento no determina que una persona pertenezca a esa confesión religiosa, el dato podrá ser tratado con la base legal del interés legítimo. Diferente sería si posteriormente a esta recopilación de datos en el fichero y entrega a la empresa de Moriarty, es esta la que, poniendo en conexión este dato, junto con otros de la misma persona, obtiene una información de carácter especialmente protegido; lo cual sería un uso malicioso de datos no incluidos en esa categoría, para obtener, por este medio, información que no están legitimados a tratar, lo que, a mi entender, derivaría únicamente en responsabilidad de la empresa.

3. CÓMO SE TRATAN ESOS DATOS (ESPECIAL ANALISIS DEL PROFILING).

Concluimos en el punto V.2 que ITAINNOVA tiene un interés legítimo que le autoriza a tratar datos personales no categorizados como especialmente protegidos, pero este interés hay que contraponerlo a los intereses, derechos y libertades fundamentales de los interesados, como ya indicamos en el punto anterior; para ello creo imprescindible observar en todo tratamiento si se lleva a cabo la elaboración de perfiles, también llamado perfilado o profiling. Esta se define en el art. 4.4 RGPD <<toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha

persona física>>

La necesidad de esta observancia deriva de que el RGPD en su Considerando 71. incide en lo siguiente: <<la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas>> además la Guía del Reglamento General de Protección de Datos para responsables del tratamiento elaborada por la AEPD, determina que la elaboración de perfiles es un tipo de tratamiento arriesgado, que conlleva un riesgo mayor que el resto de tratamientos[17], lo que nos puede llevar a pensar que la realización por parte de ITAINNOVA de este tipo de prácticas podría suponer que la contraposición entre su interés legítimo para tratar datos, y los intereses, derechos y libertades de los titulares de esos datos, le fuera desfavorable, al ser esta una práctica más arriesgada, por lo que sería necesario, si quisiésemos continuar con el perfilado, añadir mayores garantías que equilibren esa contraposición. Por ello paso a analizar si en Moriarty se llevan a cabo prácticas de perfilado.

El perfilado, se define así en las Directrices sobre la toma de decisiones automatizadas y perfilado a los fines del Reglamento 2016/679 que da el Grupo de Trabajo sobre Protección de Datos del Art. 29. (Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, article 29 data protection working party): << El perfilado se compone de tres elementos:

- Tiene que ser una forma automatizada de procesamiento;
- Debe realizarse sobre datos personales; y
- El objetivo del perfilado debe ser evaluar los aspectos personales de una persona física.

(…)

El perfilado es un procedimiento que puede implicar una serie de deducciones estadísticas. A menudo se utiliza para hacer predicciones sobre las personas, utilizando datos de diversas fuentes para inferir algo sobre un individuo, en función de las cualidades de otros que parecen estadísticamente similares.

(…)

[17] Guía del Reglamento General de Protección de Datos para responsables de tratamiento [e-Book] Madrid, Agencia Española de Protección de Datos, 2017, p. 34.

En términos generales, perfilar significa recopilar información sobre un individuo (o grupo de individuos) y evaluar sus características o patrones de comportamiento para ubicarlos en una determinada categoría o grupo, en particular para analizar y / o hacer predicciones, por ejemplo, sobre su:

- capacidad para realizar una tarea;
- intereses; o
- comportamiento probable>>[18]

Como su propio nombre indica, el perfilado, trata de obtener el perfil completo de una persona, gustos, aficiones, sexo, edad…. y posteriormente agruparla con otras de perfil similar, llevando a cabo en ellas un tratamiento automatizado en función del grupo donde han sido incluidas, con intención de analizar su comportamiento y hacer predicciones del mismo.

En Moriarty hay una parte de trabajo que ITAINNOVA llama perfilado, y aunque es posible que haya desiciones automatizadas en base a datos personales, determinamos que esto no se corresponde con el perfilado que define la ley. ITAINNOVA denomina perfilado a esta práctica debido a que hacen grupos de personas, pero esos grupos no se forman según el perfil de las mismas

---

[18] Article 29 data protection working party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017. p. 6 y 7.

<<Profiling is composed of three elements:

- it has to be an automated form of processing;
- it has to be carried out on personal data; and
- the objective of the profiling must be to evaluate personal aspects about a natural person.

(…)

Profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar.

(…)

Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their:

- ability to perform a task;
- interests; or
- likely behaviour.>>

sino según los temas de los que hablan, por ejemplo: ITAINNOVA agrupa a todos aquellos que están hablando de aceitunas, pero en esta actuación que ellos llaman perfilado no diferencian entre aquellos que hablan favorablemente y los que no, y actúan igual con el resto de condiciones, no agrupan por edades, sexo etc, simplemente por los temas de los que están hablando, sin importar lo que se dice, ni las características físicas, ni aficiones que puedan llegar a tener esos usuarios, por lo que podemos determinar que no elaboran un perfil que les permita analizar o hacer predicciones sobre las capacidades, intereses o comportamientos probables de los interesados.

Debemos aclarar que, si en algún momento, ITAINNOVA decidiera llevar a cabo prácticas de perfilado, esto no supondría obligatoriamente que el interés legítimo dejaría de servir como base legal al tratamiento; es posible que el impacto sobre los intereses, derechos y libertades de los interesados fuera mayor, pero si pudiésemos establecer las garantías necesarias para protegerlos, el interés legítimo continuaría sirviendo a ITAINNOVA como base legal para el tratamiento.

4. ALMACENAMIENTO DE LOS DATOS.

Lo primero que hace ITAINNOVA cuando la empresa encarga un tratamiento de datos es realizar un fichero personalizado para la misma, que recoge datos de interés para encontrar correlaciones o información que le ayuden en la estrategia comercial.

La definición de fichero que hace el RGPD en su art. 4 es la siguiente: <<todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica>>.

Existen, con respecto a los datos incluidos en este fichero una serie de obligaciones que nos presenta el RGPD en su art. 5.1:

<<los datos personales serán:

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»).

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).>>

Se nos plantea la duda de si es el encargado del tratamiento que crea el fichero, en este caso ITAINNOVA, o es el responsable del mismo, al que finalmente se le traspasará el fichero, el que tiene la responsabilidad de que los datos almacenados sean exactos, conservados solamente durante el tiempo necesario para llevar a cabo el fin del tratamiento y recogidos de tal forma que quede garantizada su confidencialidad, a fin de proteger los derechos y libertades de aquellos a quienes pertenecen.

En la antigua LOPD 15/1999, de 13 de diciembre, ahora derogada, se incluía, en su art. 3.d. el concepto de responsable del fichero, que se identificaba con el responsable del tratamiento <<Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.>>. En la nueva LOPDGDD y en el RGPD no existe cómo tal la figura de responsable de fichero, habiendo siendo esta absorbida por la del responsable del tratamiento, como lo muestra el art. 5.2 del RGPD diciendo que: <<el responsable del tratamiento será responsable del cumplimento de lo dispuesto en el apartado 1 y capaz de demostrarlo>>, (el apartado 1 enumera las obligaciones arriba indicadas).
Es por tanto el responsable del tratamiento, en nuestro caso la empresa contratante, quien debe cumplir con las obligaciones anteriormente citadas.

5. OTROS IMPLICADOS EN EL TRATAMIENTO DE LOS DATOS :

5.1 REDES SOCIALES DE LAS QUE SE OBTIENEN LOS DATOS:

Como ya hemos indicado en puntos anteriores, ITAINNOVA confecciona un fichero privado con datos personales obtenidos de las publicaciones que los interesados hacen en las redes sociales como Twitter y Facebook. Los Servicios de Redes Sociales (SRS) pueden definirse como <<plataformas de comunicación en linea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información>>[19]

Las redes sociales son una fuente de información pública de la que ITAINNOVA obtiene datos que posteriormente usa en Moriarty. Los Servicios de Redes Sociales no tienen porque conocer que se están tratando algunos de los datos que han sido publicados en dichas plataformas. En ocasiones las propias redes comercian con ellos, pero no estamos en ese caso, puesto que ITAINNOVA únicamente obtiene datos de perfiles públicos y no tiene obligación de comunicar a la red social el uso de los mismos. Será la red social quien deberá cuidarse de que los perfiles privados de sus usuarios no sean accesibles a un tercero como puede ser ITAINNOVA.

5.2 TITULARES DE ESOS DATOS (REFERENCIA AL DERECHO AL OLVIDO)

El Capítulo III del RGPD, habla de los derechos del interesado, enumerados de la siguiente manera:

- Derecho de acceso del interesado a los datos personales, el interesado tendrá derecho a saber si se están tratando o no datos personales qué le conciernan, y en caso afirmativo podrá acceder a sus datos personales.
- Derecho de información, el interesado tiene derecho a obtener del responsable del tratamiento la información que determina la ley.
- Derecho de rectificación, tendrá derecho a que se rectifiquen datos personales inexactos que le afecten.
- Derecho de supresión, también llamado derecho al olvido, tendrá derecho a obtener la supresión de los datos personales que le conciernan.

[19] Grupo de Trabajo del art. 29. Dictamen 5/2009 sobre las redes sociales en línea, 12 de junio de 2009, p.5

- Derecho a la limitación del tratamiento, el interesado tendrá derecho a que se limite el tratamiento de los datos cuando se den una serie de condiciones.
- Derecho a la portabilidad, tendrá derecho a transmitir los datos personales que haya facilitado a un responsable del tratamiento, a otro; sin que el primero lo impida.
- Derecho de oposición, tendrá derecho a oponerse al tratamiento de sus datos personales.

Hay tres de estos derechos que por su importancia voy a desarrollar.

A. DERECHO DE ACCESO

El derecho de acceso nos plantea la duda de si ITANNOVA debe informar a los usuarios cada vez que trata sus datos personales: entendemos que no, ya que el propio RGPD en la definición de este derecho dice lo siguiente: <<Artículo 15 Derecho de acceso del interesado 1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información.>>. No estamos hablando de una obligación de comunicar al interesado el tratamiento de sus datos personales, sino de confirmarle, en el caso de que lo solicite, que sus datos están siendo tratados.

Nos deja claro el artículo 15 que se trata de una comunicación posterior a una petición previa, ya que sin esta no puede haber confirmación. En el caso de que se confirme el tratamiento de sus datos personales, el interesado tendrá derecho de acceso a los mismos.

B. DERECHO DE INFORMACIÓN

El art. 14 del RGPD determina la información que el responsable del tratamiento debe facilitar al interesado cuando los datos personales no se hayan obtenido del mismo como es el caso de ITAINNOVA. Esta información será relativa al tratamiento de los datos del interesado, y ya hemos aclarado que ITAINNOVA y su cliente no tienen obligación de comunicarle que se están tratando sus datos personales si no existe una petición previa por su parte. Además el art. 14.5.b RGPD establece sobre el derecho de información, entre otras, la siguiente excepción: <<Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

5.b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información>>

Por tanto, teniendo en cuenta que el interesado no conoce que se están tratando sus datos y que ITAINNOVA y su cliente, de no existir petición previa, no tienen obligación de comunicárselo, supondría un esfuerzo desproporcionado trasladar esta información a todos aquellos a quienes pertenecen los datos; por lo que, solo en el caso de que exista esa petición, deberán confirmar el tratamiento de datos según el derecho de acceso, y proporcionar al interesado la información que ordena el art. 14 relativa al tratamiento de sus datos.

C. DERECHO DE SUPRESIÓN (DERECHO AL OLVIDO)

El derecho de supresión (derecho al olvido), está incluido en el art. 17 del RGPD:

<<1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
- el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
- los datos personales hayan sido tratados ilícitamente;

(…)

2. Cuando haya hecho públicos los datos personales y este obligado en virtud de lo dispuesto en el apartado 1 a, suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.…>>

El derecho al olvido, lo define la Guía del Reglamento General de Protección de Datos para Responsables del Tratamiento en su página 10, <<es una manifestación de los derechos de cancelación u oposición en el entorno online (según la jurisprudencia que el Tribunal de Justicia de la UE estableció en el caso Google Spain)>>[20], por tanto existe un derecho a solicitar la supresión de datos personales que circulan en Internet.

Podemos ver que el derecho al olvido, es en realidad el derecho de supresión referido al ámbito de la red; ejercer el derecho al olvido es solicitar el borrado de datos propios que circulan en Internet. En el caso de ITAINNOVA los datos sobre los que habría que actuar, aunque se hayan obtenido de la red, se encuentran contenidos en un fichero que no se encuentra en Internet, sino que se ha puesto a disposición únicamente del cliente, eso determina que el derecho que realmente se puede ejercer ante ITAINNOVA será el de supresión.

El derecho de supresión según el art. 17 puede ser ejercido por el interesado cuando concurra alguna de las circunstancias que el artículo menciona y que hemos reproducido arriba. La segunda circunstancia, retirada del consentimiento, no es aplicable a nuestro caso, puesto que nuestro principio de actuación es el interés legítimo, no el consentimiento que nunca hemos obtenido. Las otras circunstancias nos afectarían directamente:

La primera de ellas es que los datos ya no sean necesarios para los fines del tratamiento, y eso implicaría que los datos ya deberían haber sido eliminados del fichero por el responsable en base al principio de necesidad del tratamiento, y si no ha sido así deberá procederse a su borrado inmediato.

[20] Guía del Reglamento General de Protección de Datos para responsables de tratamiento [e-Book] Madrid, Agencia Española de Protección de Datos, 2017, p.10

La cuarta circunstancia, que los datos personales hayan sido tratados ilícitamente obliga al borrado directo por la ilegalidad de la actuación. Es la tercera circunstancia, oposición al tratamiento, la que plantea más dificultad, debido a la posibilidad de tener que realizar una ponderación de intereses entre el usuario y el responsable del tratamiento. El art. 17 establece que una de las circunstancias para ejercer el derecho de supresión es la oposición por parte del interesado al tratamiento de sus datos mediante el art. 21.

El art. 17 distingue dos circunstancias de oposición, una mediante el apartado segundo del art. 21, el cual especifica que en el caso de que el tratamiento de datos personales tenga por objeto la mercadotecnia, se otorga al interesado el derecho de oponerse en todo momento al tratamiento de los datos que le conciernan sin que sea necesario realizar una ponderación de intereses. Y otra mediante el apartado primero del artículo 21 que permite al responsable del tratamiento acreditar que tiene motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, derechos y libertades del interesado, y que no podrá aplicarse en caso de que el tratamiento tenga por objeto la mercadotecnia, al estar incluido este supuesto en el punto segundo.

Atendiendo al objeto del tratamiento que realizan ITAINNOVA y su cliente, vemos que este encaja en la definición de mercadotecnia, entendida como un conjunto de prácticas destinadas a la búsqueda de necesidades y deseos existentes en el mercado con la finalidad de satisfacerlos mejorando así la economía de la empresa que la realiza. Estaría por tanto en el ámbito de aplicación del apartado segundo del art. 21, y cualquier oposición al tratamiento implicaría que automáticamente se dejaran de tratar los datos del interesado, y este pudiese ejercer su derecho de supresión procediéndose al borrado de sus datos.

En el caso de que en algún momento, el objeto del tratamiento no fuera la mercadotecnia, se estaría en el ámbito de aplicación del apartado primero del art. 21, y este permitiría realizar una ponderación entre los intereses del responsable del tratamiento y los intereses, derechos y libertades del interesado, según el resultado de esta ponderación habrá lugar o no a la paralización del tratamiento y al ejercicio del derecho de supresión.

Por otro lado si la red social, ante una solicitud de derecho al olvido, tuviese que borrar ciertos datos, intentará, según el art. 17.2, comunicar al resto de responsables que traten con esos datos la necesidad de su eliminación. <<Los responsables que hayan hecho públicos los datos personales

deberán adoptar medidas técnicas para informar a otros responsables de la solicitud del interesado de borrar su información personal>>[21]. Pero ante la dificultad de que la red social nos informe de esta solicitud de derecho al olvido, ya que ella no conoce nuestro tratamiento de datos, seremos nosotros, en concreto la empresa, quien al actualizar los datos en aplicación del principio de exactitud y actualización de los mismos, efectuara el borrado de esos datos que ya habrán desaparecido de las redes sociales.

Por ultimo debemos determinar, qué borrar y quién debe efectuar el borrado en el caso de que alguien ejerza su derecho de supresión.

Una vez identificado el dato (por ejemplo un tweet) que tenemos que borrar, se nos plantea la duda de si ademas del borrado del mismo debemos borrar también las estadísticas en las que ha sido incluido. A mi parecer, no seria necesario borrar las estadísticas que el dato ha ayudado a generar, ya que estas no afectan en modo alguno a los intereses del usuario, puesto que el dato, al ser incluido en la estadística, se convierte únicamente en un número que no muestra información alguna del usuario. Pero si ITAINNOVA en algún momento realizase prácticas de perfilado, sí sería necesario efectuar un borrado del perfil que el dato ha ayudado a crear.

Y respecto a quién tiene la obligación de efectuar el borrado, el art. 17 del RGPD indica que será el responsable del tratamiento el encargado de efectuarlo, aunque podría delegar esta función en ITAINNOVA.

5. 3 EMPRESA QUE ENCARGA REALIZAR EL PROYECTO A ITAINNOVA

La empresa que encarga realizar el proyecto a ITAINNOVA es su cliente y, como ya hemos determinado en puntos anteriores, será el responsable del tratamiento. ITAINNOVA asume la figura de encargado del tratamiento, y cada uno de ellos tiene diferentes obligaciones y responsabilidades. Vamos a ver en este apartado varios aspectos de la relación entre ambos:

[21] Ibídem, p.10.

A. OBLIGACIONES ESPECÍFICAS PARA LOS ENCARGADOS

Anteriormente al RGPD tanto la Directiva 95/46 como las leyes nacionales se centraban en la actividad y responsabilidades del responsable del tratamiento, actualmente el nuevo RGPD contiene también obligaciones y responsabilidades dirigidas a los encargados.

- <<Deben mantener un registro de actividades de tratamiento.

- Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.

- Deben designar a un Delegado de Protección de Datos en los casos previstos por el RGPD>>[22]

Son estas las obligaciones del encargado, aunque en el caso de ITAINNOVA, la designación del Delegado de Protección no es necesaria ya que no se incluye dentro de los casos previstos por el RGPD.

Pero aunque el RGPD haya asignado obligaciones propias a los encargados, que pueden ser supervisadas separadamente de las del responsable del tratamiento por las autoridades de protección de datos, la AEPD sigue indicando lo siguiente: <<La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad>>[23].

B. CONTRATO DE ENCARGO:

Ordena el RGPD en su art. 28.3 que debe existir siempre un contrato, entre el responsable y el encargado del tratamiento <<El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable>> en él se darán las instrucciones precisas de cual debe ser la actuación del encargado del tratamiento. La Guía del Reglamento General de Protección de Datos, creada por la AEPD, desarrollando el Reglamento, determina que el contrato debe prever aspectos como los siguientes:

[22] Ibídem, p.13.

[23] Ibídem.

- <<Objeto, duración, naturaleza y la finalidad del tratamientos
- Tipo de datos personales y categorías de interesados
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados... >>[24]

Para contratos anteriores a la aplicación del RGPD, en mayo de 2018, la AEPD determina que deberán modificarse y adaptarse para respetar este contenido. Para facilitar la redacción de los contratos, la AEPD y las autoridades de protección de datos autonómicas han creado unas directrices que posibilitan la redacción de los mismos y que pueden consultarse en la Guía del Reglamento General de Protección de Datos para Responsables del Tratamiento, en el enlace al que remite en su página 15; incluyendo entre estas directrices varios modelos de contrato.

C. RESPONSABILIDADES:

A pesar de que la responsabilidad última del tratamiento recae sobre el responsable del mismo, el incumplimiento de las normas de protección de datos por parte del encargado de tratamiento, actuando independientemente del responsable del mismo, podría acarrearle ciertas responsabilidades, convirtiéndole en responsable del tratamiento para estas actuaciones, tal y como determina el art. 28.10 del RGPD <<Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento>>.

Por otro lado en el caso de que el encargado del tratamiento recibiese una instrucción contraria a las normas de protección de datos, deberá informar al responsable del tratamiento de la ilegalidad de la misma, art. 28.3 RGPD: <<En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el

[24] Ibídem.

presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros>> y no debería ejecutarla, o incurrirá en corresponsabilidad.

V. COMO DETERMINAR LA SITUACIÓN DEL PROYECTO CON RESPECTO A LA NORMATIVA ACTUAL EN MATERIA DE PROTECCIÓN DE DATOS.

Para determinar la situación del proyecto con respecto a la normativa de protección de datos, la AEPD ha creado, dentro de la Guía del Reglamento General de Protección de Datos para responsables del tratamiento, una lista de verificación con la siguiente pretensión: <<ayudar a las organizaciones a llevar a cabo de forma ordenada una valoración de su situación frente a las principales obligaciones del RGPD>>[25]. El contenido de esta lista es <<un listado de preguntas que responsables y encargados deberán formularse, y responder adecuadamente, a la hora de determinar cuál es su situación ante la aplicación del RGPD>>[26]. Estas preguntas tienen que ver con la legitimación, la información y derechos de los interesados, las relaciones entre el responsable y el encargado y las medidas de responsabilidad proactiva.

Establece la propia Guía que en ciertos casos se podrá usar para esta valoración una lista de verificación simplificada <<los responsables que realicen un número limitado de tratamientos que probablemente presenten un bajo nivel de riesgo para los derechos y libertades de los interesados, podrán simplificar la valoración de los aspectos relevantes a la hora de determinar que están en condiciones de aplicar adecuadamente el RGPD>>[27]. La posibilidad de utilizar la lista simplificada la determina la propia Guía excluyendo a los siguientes responsables: <<Esta aproximación simplificada no sería válida para responsables que, con independencia de su tamaño, desarrollen tratamientos que impliquen un nivel de riesgo mayor. Por el tipo de tratamiento (por ejemplo, elaboración de perfiles), por el tipo de datos tratados (por ejemplo, uso de datos sensibles) o por el uso de determinados medios de tratamiento (por ejemplo, tecnologías de análisis masivo de información)>>[28]. Aunque a mi entender, ITAINNOVA hace un tratamiento de bajo riesgo, usa sin embargo tecnologías de análisis masivo de información, por lo que no debería aplicar esta lista de

[25] Ibídem, p.31.

[26] Ibídem.

[27] Ibídem, p.34.

[28] Ibídem.

verificación simplificada, que parece haber sido creada para pequeñas empresas que tratan datos de sus trabajadores o de sus clientes.

Por tanto, para conocer la situación del proyecto con respecto al RGPD, ITAINNOVA y su cliente, deberán contestar las preguntas planteadas en la lista de verificación no simplificada y las respuestas a las mismas determinarán si están dentro o no de la legalidad del RGPD. Se incluye la lista de verificación, en el anexo I.

VI. CONCLUSIONES.

La razón de este trabajo es ayudar a ITAINNOVA a ajustarse al nuevo RGPD, en los proyectos de desarrollo de sistemas informáticos para el tratamiento de datos obtenidos de redes sociales usando la plataforma Moriarty. He intentado en este trabajo comprobar como se adaptan los sistemas desarrollados con Moriarty a la normativa vigente, llegando a las siguientes conclusiones:

ITAINNOVA es el encargado del tratamiento, y la empresa contratante asume la figura de responsable del mismo, con todas las responsabilidades que la ley impone a cada uno de ellos. Este tratamiento de datos, tiene como única base legal el interés legítimo, y los datos a tratar serán siempre datos personales no categorizados como especialmente protegidos, además ITAINNOVA y su cliente deberán tener en cuenta que su interés legítimo debe ser contrastado con los intereses, derechos y libertades fundamentales de los interesados.

En este tratamiento de datos no se llevan a cabo prácticas de perfilado, puesto que no hay tratamiento automatizado de datos personales con la finalidad de categorizar usuarios y predecir sus comportamientos, pero en el caso de que posteriormente se realizase esta práctica, habría que incluir ciertas garantías que protegiesen los intereses, derechos y libertades de los interesados y evitasen un impacto excesivo en los mismos.

Además de ITAINNOVA, están presentes en este tratamiento las redes sociales como proveedoras de datos, aunque ellas no tienen porque conocer nuestro uso de los mismos; los titulares de los datos, o interesados, cuyos derechos deben respetarse; y la empresa que contrata a ITAINNOVA. Respecto a los interesados, hemos analizado como más importantes el derecho de acceso, el derecho de información y el derecho de supresión, y concluido que el derecho de acceso es más un derecho

de confirmación, ya que ITAINNOVA, o la empresa contratante, deben responder únicamente previa solicitud del interesado. Que el derecho de información será de aplicación también previa solicitud del interesado, ya que cualquier otra actuación supondría un esfuerzo desproporcionado. Y por último que el derecho de supresión otorga al interesado la facultad de solicitar el borrado de sus datos siempre que se den unas circunstancias específicas; he hecho especial hincapié en la circunstancia de que el interesado se oponga al tratamiento; y determinado que, como ITAINNOVA y su cliente realizan una labor de mercadotecnia, cualquier oposición al tratamiento habilita el derecho de supresión del interesado sin que aquellos tengan opción de acreditar motivos legítimos para continuar con el tratamiento.

La relación entre ITAINNOVA y su cliente debe estar recogida en un contrato de encargo cuyo contenido regula la ley; esta misma establece que la responsabilidad final del tratamiento será siempre del responsable del mismo, al igual que la de mantener el fichero con las obligaciones de actualización, exactitud, y seguridad. La ley también crea obligaciones nuevas para encargados del tratamiento, y aclara que en el caso de que el encargado del tratamiento se extralimite en sus funciones, asumirá, para esas actuaciones, la figura de responsable del tratamiento, con todas las responsabilidades que ello conlleva; y que si ITAINNOVA recibe de su cliente instrucciones contrarias a la legalidad no deberá ejecutarlas, o de lo contrario, incurrirá en corresponsabilidad.

Por último he tratado de facilitar a ITAINNOVA y a su cliente la tarea de determinar en cualquier momento la situación de su proyecto con respecto a la normativa de protección de datos, incorporando en el anexo I la lista de verificación que propone la Guía del Reglamento General de Protección de Datos para responsables del tratamiento, elaborada por la AEPD; para que responsable y encargado puedan, respondiendo a las preguntas de la misma, verificar el cumplimiento de la ley.

Después de comprobar exhaustivamente si el tratamiento de datos que realiza Moriarty, se adapta a las normas de protección de datos; he determinado, por todo lo expuesto, que este tratamiento es legítimo y que, si se cumplen las prescripciones indicadas, será acorde con la ley. Aunque en esta materia, dada la reciente entrada en vigor del RGPD, queda mucho por desarrollar, mucha doctrina que escribir y sentencias por dictar, interpretaciones todas ellas que facilitarán enormemente la aplicación de esta nueva norma.

VII. BIBLIOGRAFÍA Y REFERENCIAS DOCUMENTALES:

1. V. MAYER - SCHÖNBERGER y K. CUKIER, Big data. La revolución de los datos masivos, Titivillus, 2013.
2. Página web de ITAINNOVA: https://www.itainnova.es/es/itainnova.
3. Grupo de Trabajo del art. 29, Dictamen 1/2010, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»,16 de febrero de 2010.
4. Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento [e-Book] Madrid, Agencia Española de Protección de Datos, 2017.
5. Grupo de Trabajo del art. 29. Dictamen 06/2014 sobre el concepto de interés legitimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, 9 de abril de 2014.
6. J. A. Messía de la Cerda Ballesteros. Actualidad Civil, Nº 5, 2018. Al que se hace referencia en https://laleydigital.laley.es. LA LEY 4473/2018.
7. J. Pérez Gil, Protección de datos y proceso penal, LA LEY, Madrid, 2010. Consultado en: laleydigital.laley.es, LA LEY 8123/2011.
8. Article 29 data protection working party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3 October 2017.
9. Grupo de Trabajo del art. 29. Dictamen 5/2009 sobre las redes sociales en línea, 12 de junio de 2009.

ANEXO I:

Lista de verificación para encargados y responsables del tratamiento:

Legitimación

- ¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?
- Si alguno de los tratamientos que realiza está basado en el consentimiento de los interesados, ¿ha verificado que ese consentimiento reúne los requisitos que exige el RGDP? En caso contrario, ¿ha previsto cómo recabar el consentimiento de forma adaptada al RGPD o ha encontrado otra base legal adecuada para esos tratamientos?

Información y derechos

- La información que se proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?
- ¿Contiene esa información todos los elementos que prevé el RGPD?
  ¿Dispone de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos? ¿Pueden ejercerse los derechos por vía electrónica?
- ¿Tiene establecidos procedimientos o mecanismos que le permitan verificar la identidad de quienes solicitan acceso o ejercen los demás derechos ARCO?
- ¿Tiene establecidos procedimientos que le permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD? ¿Ha valorado si sería necesaria la colaboración de los encargados para responder a las solicitudes de los interesados y, si es así, tiene previsto incluir esta colaboración en los contratos de encargo?
- En particular, ¿tiene previstos mecanismos para atender a posibles ejercicios del derecho a la limitación del tratamiento, de forma que los datos afectados puedan ser conservados sin ser objeto de las operaciones de tratamiento que corresponderían?
- ¿Ha valorado si los tratamientos de datos que realiza pueden ser objeto del derecho a la portabilidad? En caso, afirmativo, ¿ha previsto procedimientos o mecanismos para poder atender a este derecho y proporcionar los datos al interesado (o a otro responsable) en un formato estructurado, de uso común y susceptible de lectura mecánica?

Relaciones responsable-encargado

- ¿Ha previsto cómo valorar si los encargados con los que haya contratado o vaya a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD cuando sea de aplicación?
- ¿Contienen los contratos de encargo que actualmente tenga suscritos todos los elementos que prevé el RGPD? En caso contrario, ¿está dando pasos para adaptarlos antes de la aplicación del RGPD?

Medidas de responsabilidad proactiva

- ¿Ha hecho una valoración de los riesgos que los tratamientos que desarrolla implican para los derechos y libertades de los ciudadanos? ¿Ha determinado qué medidas de responsabilidad activa corresponden a su situación de riesgo y cómo debe aplicarlas?
- ¿Ha previsto cómo establecer el registro de actividades de tratamiento en su organización?
- ¿Ha valorado si le es de aplicación alguna de las excepciones a esta obligación?
- ¿Ha previsto quién se encargará de mantener actualizado el registro?
- ¿Ha revisado las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos? ¿Considera que puede seguir aplicando las medidas de seguridad previstas en el Reglamento de la LOPD? ¿Ha valorado suficientemente la posibilidad de introducir medidas adicionales en función del tipo de tratamiento o del contexto en que se realiza?
- Atendiendo al tipo de tratamientos que realiza, ¿ha establecido mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos?
- ¿Tiene previstas medidas de reacción frente a los diferentes tipos de quiebras de seguridad, incluidos los procedimientos para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados? ¿Ha establecido procedimientos para notificar las violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados?
- ¿Dispone de un registro o herramienta similar en que pueda documentar los incidentes de seguridad que se produzcan, aunque no sean notificados a las autoridades de protección de datos?

- ¿Ha valorado si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?
- ¿Dispone de una metodología para la realización de la Evaluación de Impacto?

  Según el tipo de tratamiento que realiza y los resultados del análisis de riesgos previo, ¿tiene
- que nombrar un Delegado de Protección de Datos?
- ¿Ha establecido los criterios para seleccionar al Delegado de Protección de Datos y, en particular, para valorar sus cualificaciones profesionales y sus conocimientos?
- El puesto de DPD tal y como está configurado en su organización, ¿respeta los requisitos de independencia en el ejercicio de las funciones, posición en el organigrama, ausencia de conflicto de intereses y disponibilidad de los recursos necesarios establecidos por el RGPD?
- ¿Ha hecho pública la designación del DPD y sus datos de contacto y los ha comunicado a la autoridad de protección de datos?
- ¿Ha establecido procedimientos para que los interesados contacten con el DPD?